UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/631,989	07/31/2003	Bjorn Markus Jakobsson	EMC-06-463	2203

80167 7590 12/09/2008

Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
12/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/631,989	JAKOBSSON ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 September 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the Applicant's Remarks and Amendments filed September 29, 2008.

Claims 1, 28, 29, and 30 are amended.

Claims 1-30 are pending and herein considered.

Response to Arguments

Applicant's arguments with respect to the rejection(s) of claim(s) 1-30 under have been fully considered but are not persuasive.

In response to Applicant's first set of arguments concerning Ginter's alleged failure to teach or suggest "the association of particular nodes of a graph with one of a number of distinct portions of partitioned cryptographic functionality" as claimed in claim 1, the Examiner respectfully disagrees. The Examiner would like to refer back to those portions sited in her previous office action, particularly paragraphs 73 and 74 wherein Ginter discloses system and method for secure transaction management and electronic rights protection including "an integration of cryptographic and other security technologies (e.g. encryption, digital signature, etc)." It is based upon this portion of the reference in view of the reference in its entirety that the Examiner maintains that Ginter does in fact disclose the cryptographic functionality as claimed by Applicant. Next, the Examiner would like to draw attention to Ginter's Abstract wherein he discloses "secure distributed ad other operating system environments and architecture, employing, for example, secure semiconductor processing arrangements that may establish secure,

protected environments at each node." Ginter goes on to teach how "these technologies may be used to support an end-to-end electronic information distribution capability." In paragraph 6 Ginter goes on to discuss his invention's relation to distributed and other operating system environments and architectures as well as secure architectures, including, for example, tamper resistant hardware-based processors, that can be used to establish security at each node of a distributed system. It is based upon these portions in view of the reference in its entirety, that the Examiner maintains that Ginter does in fact disclose the association of particular nodes of his distributed system with portions of a distributed cryptographic functionality.

In response to Applicant's next set of arguments concerning Ginter's alleged failure to teach or suggest "the transmission of information representative of one of more of such nodes from a delegating device to a recipient device so as to configure the recipient device for authorized executions of a portion of the partitioned cryptographic functionality" as claimed in claim 1, the Examiner respectfully disagrees. The Examiner would first like to refer to those arguments presented above for support regarding Ginter's teaching of nodes and partitioned cryptographic functionality. Next, the Examiner would like to draw attention to paragraphs 112-120, wherein Ginter discloses "secure metering means," "secure distributed database means for storing control and usage related information," "secure electronic appliance control means," and "a distributed, secure, "virtual back box comprised of nodes located at every user (including VDE content container creators, other content providers, client users, and recipients of secure VDE content usage information)." Ginter goes on to discuss how

the nodes of this "virtual black box" normally includes a secure subsystem having at least one secure hardware element, said secure subsystems being distributed at nodes along the path of information. Ginter even goes so far as to disclose secure communication means employing authentication, digital signing, and encrypting transmissions wherein the secure subsystems at the user nodes utilized protocols that establish and authenticate each node, as well a establishing one or more secure host-to-host encryption keys for communication between the subsystems. Last but certainly not least, the Examiner would like to draw attention to paragraph 134 of Ginter wherein he discloses the decomposition of generalized requirements for supporting electronic commerce and data security into a broad range of constituent "atomic" and higher level components that may be variously aggregated together to form control methods for electronic commerce applications and data security arrangements. This provides a secure operating environment employing foundation elements along with secure independently deliverable components that enable electronic commerce models and relationships to develop. This system specifically supports the unfolding of distribution models in which content providers, over time, can expressly agree to or allow subsequent content providers and or users to participate in shaping the system. Meanwhile, Ginter goes on in paragraph 135 to discuss the use of containers to securely transmit information among nodes of the environment, wherein those containers may be employed both for control instructions and information as well as the encapsulate electronically distributed content. It is based on the abovementioned arguments in view of the reference in its entirety, that the Examiner maintains that

Ginter provides for the transmission of information representative of one or more nodes and their cryptographic functionality, from delegating devices to recipient devices wherein the information transmitted may be used to configure the recipient device, more often than not an addition to the distribution community invited in by an existing member, so that the new recipient device may be authorized for execution of a portion of the cryptographic functionality. As such, the Examiner maintains that Ginter does in fact teach "transmitting from the delegating device to the recipient device information representative of one or more of the nodes wherein the recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality" as claimed by Applicant in claim 1.

In response to Applicant's remarks concerning the patentability of dependent claims 2-27 based on their dependence on claim1, the Examiner respectfully disagrees, maintaining her rejection of claims 2-27 for those reasons given above in view of her previous rejection.

In response to Applicant's remarks concerning his amendments to claims 1 and 27-30, it is the Examiner's position that Ginter teaches each of Applicants newly added limitations. Her rejection of each of these newly added limitations may be found below.

In view of the remarks made above, in view of the reference in its entirety, the Examiner has no choice but to maintain her rejection of claims 1-30 under 35 USC 102(e) as anticipated by Ginter. These rejections have been included below in a form to reflect Applicant's amendments.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Applicant's newly added claim limitations include the addition of nodes corresponding to "respective seeds" wherein "a first seed associated with a node of a first one of the levels is computer as a function of a second seed associated with a node of a second one of the levels higher than the first level" and wherein "the transmitted information including the first seed but not the second seed." While this may not be the first time that Applicant has mentioned seed within his claims (see claim 22), this particular mention fails to provide the necessary structural relationship between these seeds and his underlying system. While it is true that the Examiner found no need to object to claim 22 which provides for "an ability to compute one or more seeds," newly amended claim 1 provides no such relationship. Rather, claim 1, upon which claim 22 relies, calls for "respective seeds" without having ever mentioned the creation of seeds and without clearing up whether or not the "respective seeds" in claim 1 are actually the same seeds as claim 22, but more numerous, or whether the "respective seeds" are entirely distinct and separate from the "one or more seeds" computed in dependent claim 22. If it is Applicant's intention to claim the ability to computer one or more seeds,

of which respective seeds correspond to particular nodes, Applicant is required to amend claims 1, 22, 28, 29 and 30 accordingly. As such, the Examiner has chosen to treat Applicant's "respective seeds" equivalent to the "one or more seeds" computed in claim 22 and has rejected them accordingly.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-30 are rejected under 35 U.S.C. 102(e) as being anticipated by United States Patent Application Publication No. 2007/0226807 A1 to Ginter et al.

As per **claim 1**, Ginter teaches a method for partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes, the method comprising the steps of (pars 73-74):

associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality (pars 74, 92); and

transmitting from the delegating device to the recipient device information representative of one or more of the nodes (pars 110, 112),

the recipient device being configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality (pars 74, 1114, 2187);

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level (pars 134-145);

wherein the nodes correspond to respective seeds (pars 610, 1452, 1519, 1521);

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level (pars 610, 1452, 1519, 1521);

the transmitted information including the first seed but not the second seed (pars 134-145).

As per **claim 2**, Ginter teaches wherein at least one of the nodes of the graph corresponds to a seed the possession of which permits execution of a corresponding one of the distinct portions of the cryptographic functionality (pars 610, 1452, 1519, 1521).

As per **claim 3**, Ginter teaches wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least two of the nodes (pars 74, 92, 1548, 2099, 2240).

As per **claim 4**, Ginter teaches wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least one parent node of the graph (pars 2142, 2257, 2258, 2263).

As per **claim 5**, Ginter teaches wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least one child node of a parent node of the graph (pars 2142, 2257, 2258, 2263).

As per **claim 6**, Ginter teaches wherein the graph comprises at least first and second root nodes (pars 2142, 2257, 2258, 2263).

As per **claim 7**, Ginter teaches wherein the graph comprises a tree having at least first and second subtrees associated with respective first and second ones of the plurality of distinct portions of the cryptographic functionality (pars 590, 1548, 2099, 2240).

As per **claim 8**, Ginter teaches wherein the graph comprises a chain (pars 59, 83, 107, 137, 148, 181, 189).

As per **claim 9**, Ginter teaches wherein the graph comprises L levels of nodes, an Lth one of the levels comprising a parent node v.sub.L,1, and a first one of these levels comprising a set of seeds v.sub.1,1, v.sub.1,2, . . . v.sub.1,n, where n is the total number of seeds, each of the seeds being derivable from the parent node (pars 610, 1452, 1519, 1521).

As per **claim 10**, Ginter teaches wherein an ith node of a kth one of the levels is computed as f.sub.k(i, v.sub.k+1), where f.sub.k is a one-way function (pars 610, 1452, 1519, 1521).

As per **claim 11**, Ginter teaches wherein the nodes of one or more of the levels are arranged in the form of tuples of designated numbers of nodes (pars 610, 1452, 1519, 1521).

As per **claim 12**, Ginter teaches wherein the ith node of a jth tuple of the kth level is computed as f.sub.k(j, i, v.sub.k+1,j) (pars 610, 1452, 1519, 1521).

As per **claim 13**, Ginter teaches wherein the cryptographic functionality comprises a cryptographic functionality provided by a hardware-based authentication token (pars 74, 1114, 2187).

As per **claim 14**, Ginter teaches wherein the cryptographic functionality comprises an ability to verify at least one of an authentication code and a distress code generated by a hardware-based authentication token (pars 74, 1114, 2187).

As per **claim 15**, Ginter teaches wherein the authentication token is configured to store at least two seeds, and the cryptographic functionality comprises a verification operation performed collaboratively by at least first and second servers each storing one of the seeds (pars 510, 1452).

As per **claim 16**, Ginter teaches wherein the cryptographic functionality comprises an ability to generate at least one of an authentication code and a distress code utilizing a hardware-based authentication token (pars 74, 1114, 2187).

As per **claim 17**, Ginter teaches wherein the cryptographic functionality comprises at least one of an ability to verify a signature and an ability to generate a signature (pars 74, 169, 572, 1114).

As per **claim 18**, Ginter teaches wherein the cryptographic functionality comprises an ability to generate one or more values of a one-way chain (pars 59, 83, 107, 137, 148, 181, 189).

As per **claim 19**, Ginter teaches wherein the cryptographic functionality comprises an ability to perform symmetric cryptographic operations (pars 1452, 1518-1525).

As per **claim 20**, Ginter teaches wherein the cryptographic functionality comprises an ability to perform asymmetric cryptographic operations (pars 503-505, 1452, 1518-1525) .

As per **claim 21**, Ginter teaches wherein the cryptographic functionality comprises an ability to derive one or more cryptographic keys (pars 503-505, 1452, 1518-1525).

As per **claim 22**, Ginter teaches wherein the cryptographic functionality comprises an ability to compute one or more seeds (pars 610, 1452, 1519, 1521).

As per **claim 23**, Ginter teaches wherein at least one of the seeds corresponds to at least one of the nodes of the graph (pars 510, 1452, 1519, 2521).

As per **claim 24**, Ginter teaches wherein the cryptographic functionality is partitioned in accordance with a subscription model which requires compliance with at least one specified criterion for transmission from the delegating device to the recipient device of the information representative of one or more of the nodes (pars 1548, 2099, 2240).

As per **claim 25**, Ginter teaches wherein compliance with the specified criterion is satisfied upon receipt of a designated payment (pars 16-18,1775).

As per **claim 26**, Ginter teaches wherein the recipient device and the delegating device collaborate to perform at least one of a cryptographic verification function and a cryptographic generation function (pars 918, 1519, 1626, 1673, 1775).

As per **claim 27**, Ginter teaches wherein the recipient device includes only a limited computational ability associated with performance of the cryptographic function (pars 225, 471, 473, 1698).

As per **claim 28**, Ginter teaches an apparatus comprising:

a processing device comprising a processor coupled to a memory (pars 225, 471, 473, 1698)

the processing device being utilized in conjunction with partitioning of cryptographic functionality ***so as to permit*** delegation of at least one of a plurality of

distinct portions of the cryptographic functionality from the processing device, configured as a delegating device, to at least one recipient device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes (pars 74, 92);

the processing device being configured to associate a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and to transmit to the recipient device information representative of one or more of the nodes (pars 74, 92);

the recipient device being configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality (pars 74, 1114, 2187);

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level (pars 134-145);

wherein the nodes correspond to respective seeds (pars 610, 1452, 1519, 1521);

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level (pars 610, 1452, 1519, 1521);

the transmitted information including the first seed but not the second seed (pars 134-145).

As per **claim 29**, Ginter teaches an apparatus comprising: a processing device comprising:

a processor coupled to a memory (pars 225, 471, 473, 1698);

the processing device being utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality to the processing device, configured as a recipient device, from at least one delegating device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes (pars 73-74);

a given set of the nodes being associated with a corresponding one of the plurality of distinct portions of the cryptographic functionality (pars 74, 92; the processing device being operative to receive from the delegating device information representative of one or more of the nodes (pars 110, 112),

the processing device being configured based on the received information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality (pars 74, 1114, 2187);

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level (pars 134-145);

wherein the nodes correspond to respective seeds (pars 610, 1452, 1519, 1521);

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level (pars 610, 1452, 1519, 1521);

the transmitted information including the first seed but not the second seed (pars 134-145).

As per **claim 30**, Ginter teaches a machine-readable storage medium containing one or more software programs for use in partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes, wherein the one or more software programs when executed by the delegating device implement the steps of:

associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality (pars 74, 92); and

transmitting from the delegating device to the recipient device information representative of one or more of the nodes (pars 110, 112),

the recipient device being configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality (pars 74, 1114, 2187);

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level (pars 134-145);

wherein the nodes correspond to respective seeds (pars 610, 1452, 1519, 1521);

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level (pars 610, 1452, 1519, 1521);

the transmitted information including the first seed but not the second seed (pars 134-145).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437